Un théorème de Goldbach pour les polynômes à coefficients entiers

D. R. Hayes
Université du Tennessee

La conjecture de Goldbach affirme que tout entier supérieur à 2 est la somme de deux nombres premiers. Soit $\mathbb{Z}$ l'ensemble des entiers relatifs. Le domaine polynomial $\mathbb{Z}[x]$ est, comme $\mathbb{Z}$, un domaine à factorisation unique pour lequel les polynômes irréductibles jouent le rôle des nombres premiers. Notre objectif dans cette note est de démontrer l'analogue suivant de la conjecture de Goldbach pour le domaine $\mathbb{Z}[x]$:

Théorème 1. *Pour tout polynôme M dans $\mathbb{Z}[x]$ de degré $n \geq 1$ il existe des polynômes irréductibles A et B, chacun de degré n, tels que $A + B = M$.*

On a besoin du lemme suivant.

Lemme. *Soient p et q des nombres premiers impairs distincts. Alors existent des entiers c et d tels que $p \nmid c$ et $q \nmid d$ et $pc + qd = 1$.*

Preuve. Dans la théorie élémentaire des nombres, on sait qu'existent des entiers c_0 et d_0 tels que $pc_0 + qd_0 = 1$. Si $p \nmid c_0$ et $q \nmid d_0$, alors il n'y a rien à démontrer. Supposons, alors, comme on le peut, que $p \mid c_0$. Si $c_r = c_0 + qr$ et $d_r = d_0 - pr$, alors clairement, pour tout entier r, $pc_r + qd_r = 1$. Maintenant, ni c_1 ni c_2 ne sont divisibles par p. Sinon, en considérant les différences $c_1 - c_0$ et $c_2 - c_0$, on pourrait déduire que $p \mid q$. Aussi, l'un des deux nombres d_1 et d_2 n'est pas divisible par q. Sinon, q devrait diviser $d_1 - d_2 = p$. L'une des paires (c_1, d_1) et (c_2, d_2), par conséquent, satisfait les conditions du lemme. Cela complète la preuve.

Preuve du théorème 1. Supposons que $M = m_0x^n + m_1x^{n-1} + \ldots + m_n$. Choisissons des nombres premiers impairs distincts p et q qui ne divisent ni m_0 ni m_n, et choisissons a'_0 et b'_0 tels que $qa'_0 + pb'_0 = m_0$. Posons $a_0 = qa'_0$ et $b_0 = pb'_0$. Alors

$$m_0 = a_0 + b_0, \quad p \nmid a_0, \quad q \nmid b_0. \tag{1}$$

Pour tout $0 < i < n$, choisissons a'_i et b'_i tels que $pa'_i + qb'_i = m_i$. Posons $a_i = pa'_i$ et $b_i = qb'_i$. Alors, pour $0 < i < n$,

$$m_i = a_i + b_i, \quad p \mid a_i, \quad q \mid b_i. \tag{2}$$

Par le lemme, choisissons a'_n et b'_n tels que $pa'_n + qb'_n = m_n$ mais $p \nmid a'_n$ et $q \nmid b'_n$. Posons $a_n = pa'_n$ et $b_n = qb'_n$. Alors

$$m_n = a_n + b_n, \quad p \mid a_n, \quad p^2 \nmid a_n, \quad q \mid b_n, \quad q^2 \nmid b_n. \tag{3}$$

The American Mathematical Monthly, Vol. 72, No. 1 (Jan., 1965), pp. 45-46, publié par l'Association mathématique américaine (MAA).

Si $A = a_0x^n + a_1x^{n-1} + \ldots + a_n$, et si $B = b_0x^n + b_1x^{n-1} + \ldots + b_n$, alors (1), (2) et (3) montrent que $A + B = M$ et que A et B sont des polynômes de Eisenstein. Puisque de tels polynômes sont irréductibles ([2], p. 74), La preuve est complète.

Le théorème 1 est un cas particulier du théorème suivant plus général :

THÉORÈME 2. *Soit* $\boldsymbol{R}$ *un domaine idéal principal (voir [1], p. 151) qui contient une infinité d'éléments premiers. Pour tout polynôme* M *dans* $\boldsymbol{R}[x]$ *de degré* $n \geq 1$*, il y a des polynômes irréductibles* A *et* B*, chacun de degré* n*, tels que* $A + B = M$.

La preuve du théorème 1 peut être adaptée pour démontrer ce résultat plus général. Il découle du théorème 2, par exemple, que l'analogue de la conjecture de Goldbach est vrai pour le domaine des polynômes à deux indéterminées sur un corps arbitraire.

Travail financé en partie par la subvention NSF G 16485.

Références

1. C. C. MacDuffee, Introduction to Modern Algebra, Wiley, London, 1940.

2. B. L. van der Waerden, Modern Algebra, Ungar, New York, 1949.